SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Journal of International Law

Volume 42 | Issue 3

2010

Washington and CCTV: It's 2010, Not Nineteen Eighty-Four

Aileen B. Xenakis

WASHINGTON AND CCTV: IT'S 2010, NOT NINETEEN EIGHTY-FOUR

Aileen B. Xenakis[*]

Washington, D.C.'s Closed Circuit Television (CCTV) program and the role it plays in homeland security and law enforcement can inform other jurisdictions in their development of CCTV policies and implementation. Examining both the process by which Washington, D.C. established its CCTV program and the regulations governing it yields a comprehensive understanding of the practical issues as well as constitutional issues that arise when balancing security, privacy rights, and government transparency. Analyzing strategies of successful jurisdictions, preparing to address the comments those jurisdictions received, and identifying the gaps remaining will improve the efficacy of developing CCTV programs. For an effective, efficient CCTV program that reinforces people's faith in government, departments must draft regulations that clearly articulate their end goal as well as the means they plan to use to achieve it.

I. INTRODUCTION

This article identifies best practices for creating successful Closed-Circuit Television (CCTV) programs, as well as areas to be further examined in order to implement CCTV technology and policy most effectively. Additionally, this article identifies the legal issues that arise as CCTV technology develops more quickly than the law and provides analysis of regulations governing the existing CCTV program in Washington, D.C. By sharing best practices, analyzing the comments and concerns about CCTV technology generated in other jurisdictions, and tailoring regulations to individual programs, government agencies can create successful CCTV pro-

[*] Aileen B. Xenakis is a Senior Law and Policy Analyst at the University of Maryland Center for Health and Homeland Security (CHHS). While at CHHS, Ms. Xenakis has served as a regional planner at the D.C. Homeland Security and Emergency Management Agency (HSEMA), contributing to the 2009 D.C. Presidential Inauguration Committee, the District Response Plan, and projects for both the policy and planning divisions. With the HSEMA Senior Policy Advisor and the D.C. Office of the Attorney General, Ms. Xenakis supervised a proposed rulemaking regarding the operation of D.C.'s Video Interoperability for Public Safety (VIPS) program. On behalf of HSEMA, Ms. Xenakis responded to citizens' and organizations' comments on the proposed rule, and amended the proposed rule accordingly. Additionally, she prepared briefing papers on the proposed rule and its implications for the HSEMA Director and the D.C. Mayor's Office. Ms. Xenakis is a 2007 graduate of the University of Maryland School of Law, and she graduated *magna cum laude* from Mount St. Mary's College in 2004 with a B.A. in French and English.

grams that make the community safer without sacrificing transparency, civil liberties protections, or faith in government. This essential transparency can be achieved by (1) drafting clear, straightforward regulations that reflect sensitivity to CCTV technology's potential to be misused; and (2) including added protections to assuage concerns.

II. CCTV GENERALLY

CCTV programs are becoming the next stage in law enforcement technology. Police departments have, with increasing frequency, placed agency-owned cameras in public areas and streamed the cameras' video feeds to an observation room, where police department employees can view multiple screens and see multiple areas of the city at the same time.[1] CCTV technology allows an agency employee to be effectively in two places at once—or more than two—and to observe what might otherwise require five or ten officers.[2]

CCTV programs increase efficiency in two critical ways: (1) by conserving law enforcement finances; and (2) by decreasing officers' reaction time. First, it is less expensive to pay one officer to view multiple screens and then, during an incident, contact officers in the area of the incident to respond, than to place an officer on every street corner, or even on every corner where a camera is located (which would be prohibitively expensive). Even then, officers on the street would need to rely on being in the right place at the right time whereas the cameras are constantly present. Second, CCTV can decrease the response time necessary to arrive at the scene and begin addressing an incident. This allows officers to respond quickly because they know precisely where to go without having to be in the right place at the right time to observe the initiation of an incident. CCTV also greatly reduces the miscommunication that is possible when relying on 911 operators, dispatchers, or others involved in relaying time-sensitive messages. The benefit of improved communication is enhanced when multiple agencies view their CCTV footage in the same room, often called a fusion center.[3]

---

1 *See, e.g.*, William M. Bulkeley, *Chicago's Camera Network Is Everywhere*, WALL ST. J., Nov. 17, 2009, at B7 (describing how a "giant web of video-surveillance cameras has spread across Chicago.").

2 In response to why the Washington, D.C. police began using CCTV cameras to watch live images instead of using the cameras solely as an "investigative tool," Washington, D.C.'s Chief of Police "Lanier said that she took action last fall after officials mapped locations of shootings in the city and realized that the gunfire often was taking place within range of the cameras." Allison Klein, *Police Go Live Monitoring D.C. Crime Cameras*, WASH. POST, Feb. 11, 2008, at A1.

3 According to the U.S. Department of Justice:

Fusion centers operate on a principle of efficiency that serves a broader purpose than traditional law enforcement. To gain situational awareness[4] or a common operating picture,[5] a city would purchase compatible cameras for each agency, for example, the same kind of cameras made by the same company for the jurisdiction's transportation department, school system, or emergency management, and send the video feeds from all of those cameras to one room. This room, a fusion center, is where employees from those agencies monitor multiple video feeds.

Fusion centers allow for immediate communication among employees of various agencies, thereby minimizing confusion and response time. For example, if a transportation department camera reveals an automobile accident threatening human life, the transportation employee can immediately communicate this information to a fire and emergency medical services representative, who can begin his agency's notification and response chain. By monitoring the video feed, agency employees can provide real-time information to assist first responders in making the best decisions. This preferred outcome cannot happen without immediately available information.

CCTV programs garner much attention from city governments, in particular because of their promise of efficiency and effectiveness. Though some opponents argue that cameras may just displace crime,[6] this displace-

---

> A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources.

U.S. DEP'T OF JUSTICE, FUSION CENTER GUIDELINES: DEVELOPING AND SHARING INFORMATION AND INTELLIGENCE IN A NEW ERA (EXECUTIVE SUMMARY) 3 (Apr. 2006), *available at* http://www.iir.com/global/products/fusion_center_executive_summary.pdf.

[4] Situational awareness:

> [R]efers to the capability to maintain a constant vigil over important information, understand the relationship among the various pieces of information monitored, and project this understanding into the near future to make critical decisions. In many ways the term "Situational Awareness" is, in reality, a form of mental bookkeeping.

Carlos Comperatore & William Abernathy, *Situational Awareness: What Is It?*, *in* U.S. COAST GUARD, CREW ENDURANCE MANAGEMENT 1 (Summer 2008), http://www.uscg.mil/hq/cg5/cg5211/docs/CEMSnlpubs/Vol_5_Issue2.pdf.

[5] "The Common Operational Picture . . . provides the integrated capability to receive, correlate, and display a common tactical picture, including planning applications and theater-generated overlays and projections that may include location of friendly, hostile, and neutral units, assets, and reference points." U.S. Joint Forces Command, Situational Awareness Fundamentals—Common Operational Picture, http://www.jfcom.mil/about/fact_safcop.html (last visited Mar. 11, 2010).

[6] *See generally* Sam Waples et al., *Does CCTV Displace Crime?*, 9 CRIMINOLOGY & CRIM. JUST. 207 (2009). *See also* NEW YORK CIVIL LIBERTIES UNION, WHO'S WATCHING?

ment is, in fact, a very effective disruption of crime. The urban crime arising out of illegal narcotics sales and exchanges is driven by unofficial jurisdictions, or territories, occupied by certain dealers.[7] By displacing a transaction even one block, CCTV cameras disrupt the flow of criminal commerce and prevent criminals from establishing comfortable rhythms and patterns.[8] Additionally, general and wide-spread knowledge of cameras, including but not limited to the government's posting of the cameras' locations, serves two critical functions: it deters crime[9] and it inspires confidence in the government's ability to serve and protect its residents, workers, commuters, and tourists.[10]

III. SHARING BEST PRACTICES FOR CCTV PROGRAMS

When developing CCTV programs and policies, examining the programs in other cities, including Baltimore and London, reveals which strategies are most effective in accomplishing different goals. Examining other city's programs is the first step in developing a city's own CCTV policies. Many other cities have developed and implemented CCTV programs, and each city has developed its system differently depending on the city's individual goals. Analyzing the differences and benefits other cities provide through their CCTV programs is crucial for identifying a city's own objectives and designing an effective program to accomplish them.

VIDEO CAMERA SURVEILLANCE IN NEW YORK CITY AND THE NEED FOR PUBLIC OVERSIGHT (2006) [hereinafter NYCLU REPORT], *available at* http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf (citing U.S. GEN. ACCOUNTING OFFICE, GAO/03-748, VIDEO SURVEILLANCE: INFORMATION ON LAW ENFORCEMENT'S USE OF CLOSED-CIRCUIT TELEVISION TO MONITOR SELECTED FEDERAL PROPERTY IN WASHINGTON, D.C. 29 (2003) [hereinafter VIDEO SURVEILLANCE] ("There is general consensus among CCTV users, privacy advocates, researchers, and CCTV industry groups that there are few evaluations of the effectiveness of CCTV in reducing crime . . . .")).

7 "[Cameras] provide an unquantifiable benefit—drug dealers, for example, prefer not to do business directly in front of a surveillance device. So when they walk one block away from the camera to deal on a different corner, they've lost home-turf advantage." Arthur Delaney, *The Watchmen: How Useless are the D.C. Police Department's Crime Cameras?*, WASH. CITY PAPER, Feb. 11, 2009, http://www.washingtoncitypaper.com/display.php?id=36798 (quoting D.C. police union boss Kris Baumann).

8 *See id.*

9 This argument generates much debate; very few studies have been published and very few statistics are available because few jurisdictions keep data to demonstrate the effectiveness of their CCTV systems. Opponents argue that there is no way to substantiate this argument in support of CCTV programs' implementation. *See* VIDEO SURVEILLANCE, *supra* note 6, at 29–30.

10 Citizens in the most crime-ridden neighborhoods, the neighborhood watches, etc., are big fans of this program. "'Regular citizens want those crime cameras up,' says D.C. police union boss Kris Baumann, who never hesitates to criticize the department." Delaney, *supra* note 7.

Part of Baltimore's pilot CCTV program focused on utilizing a small number of cameras concentrated in the city's downtown economic and tourism hub.[11] By publicizing the program and posting large signs within monitored areas, Baltimore achieved its goal to discourage—or at least displace—crime, and to reassure tourists that it is safe to shop and dine in the area.[12] Baltimore's goal was to deter crime and to solve more cases,[13] but, because cameras were concentrated in the downtown area, some argued that it just displaced crime.[14]

---

[11] *See* Scott Weaver, *Looking into Baltimore, London Cameras*, CHARLOTTESVILLE NEWS & ARTS, July 10–16, 2007, http://www.c-ville.com/index.php?cat=141404064434008&ShowArticle_ID=1143090707369 1218.

> It started small in Baltimore in 1996, just 16 black-and-white cameras bolted to light poles and buildings, staring straight down on a single spot, unblinking. But after a 2005 trip to London—a city 200,000-cameras strong—then-Baltimore mayor Martin O'Malley implemented City Watch. It's a city-wide network of full-color closed circuit television (CCTV) cameras that pan, zoom, tilt and are actively monitored by police. . . . Cameras were first installed to fight property crime and car theft, but even though no one was actually watching, crime dropped 10 to 15 percent.

Id.

[12] *See generally id.*; John Buntin, *Long Lens of the Law*, GOVERNING, May 1, 2009, http://www.governing.com/article/long-lens-law.

[13] Buntin, *supra* note 12.

[14] *See* Justin Fenton, *Baltimore, Britain, and the Eyes of the Law*, BALTIMORE SUN, Dec. 31, 2009, http://articles.baltimoresun.com/2009-12-31/news/bal-te.cameras31dec31_1_cameras-cctv-baltimore-sun-sent-police.

> Five years after launching a system that cost at least $5 million and continues to grow, Baltimore claims successful results—but is still trying to work out the kinks. [Westminster city coordination manager] McAlister gives former Mayor Martin O'Malley high praise for his research into CCTV and says Baltimore went big, buying some of the highest-quality equipment available at the time. With about 500 city-controlled cameras today, Baltimore has nearly as many per capita as Britain. But he is critical of the way Baltimore implemented the cameras. He said cameras were erected in the middle of problem areas, which seemed to make sense. But it sent drug dealers scattering, and police scrambling to build new intelligence. Meanwhile, pushing dealers to new corners led to an increase in turf battles—effectively stoking more crime that police were less prepared to combat. . . . Since a central watch center opened in December 2008, cameras have aided in 1,600 arrests, about half of them in the downtown business district—a 22 percent increase from the prior year. A yet-to-be-published study by the Urban Institute credits cameras with a drop in downtown crime, though it also notes an increase in violent crime in a buffer area just beyond view of the lens. "While there are mixed feelings about whether or not displacement occurs as a result of cameras, many feel that Baltimore is reaching a point of camera saturation so that there are very few places left to which criminals can displace," concluded the researcher, Nancy G. La Vigne.

Id.

Conversely, London's goal is a complete view of the entire city at all times. London boasts the largest and most extensive CCTV program in the world, with over 500,000 cameras.[15] As a capital city, London employs many cameras in all areas of the city in order to improve situational awareness. The program's extensiveness makes the CCTV program efficient, both cost-wise and in delivering safety, since a government cannot justify investing money and employee efforts in a system that is not large enough to capture the activities that pose a threat. CCTV expenditures and research will be fruitless if government employees use CCTV to observe a crime and then lose their lead as soon as the activity moves out of the scope of the cameras.

Baltimore's and London's programs heavily influenced Washington, D.C.'s plans for its CCTV program and policy. Washington, D.C.'s finished product presents a unique case study; other jurisdictions examining the way D.C. constructed its CCTV program will find both the successful elements of D.C.'s program as well as the outstanding issues yet to be addressed. The Washington, D.C. case study illustrates how important it is to identify a CCTV program's purpose clearly and transparently, and to draft regulations that are tailored to achieve that purpose while protecting civil liberties from being compromised.

IV. WASHINGTON, D.C.'S CCTV PROGRAM

Washington, D.C.'s CCTV program, also called the Video Interoperability for Public Safety (VIPS) program,[16] is a benchmark in CCTV policymaking, and the process by which the city has developed and implemented its CCTV program can inform other jurisdictions as they develop their own CCTV programs. Washington, D.C. provides an excellent example of tailoring a CCTV program and using CCTV technology to meet a city's unique needs.

Other jurisdictions may look to the process by which D.C. established its CCTV program to create a checklist of sorts to understand better the impact that a CCTV program has on stakeholders. For example, CCTV cameras are typically placed in strategic areas, but cameras may need to be moved or added if new building structures block camera feeds from viewing certain areas, assets, or infrastructure. Depending on the jurisdiction, this may implicate the city's building code and various other areas of legislation

---

[15] Michael Greenberger, *The Need for Closed Circuit Television in Mass Transit Systems*, LAW ENFORCEMENT EXECUTIVE F. 151, 152 (2006), *available at* http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=340636 (citing Ken Rodriguez , *We're Caught in Camera's Eye More Often Than You Realize*, SAN-ANTONIO EXPRESS NEWS, July 31, 2005, at 3A; *Ready for Your Closeup*, PITTSBURGH POST-GAZETTE, Aug. 25, 2005, at B7 (editorial)).

[16] Press Release, District of Columbia, Mayor Fenty Launches VIPS Program; New System Will Consolidate City's Closed-Circuit TV Monitoring (Apr. 8, 2008), http://www.dc.gov/mayor/news/release.asp?id=1273.

and regulation. There may be different legal procedures for requiring new building owners to outfit their structures with compatible video feeds or allowing the government to place cameras on the new building. This is just one of several peripheral issues affecting the success of a CCTV program. Jurisdictions that are just developing new programs can anticipate these issues by looking to other programs, such as Washington, D.C.'s, that came before theirs. Though there is certainly something to be gained by examining London's program, which is the largest and oldest CCTV program in the world and has proven success,[17] it cannot serve as the only program to inform American cities' policies because of the different privacy laws that exist in the U.K.

A. Why Washington, D.C. Is an Ideal Model for Other Cities

First, Washington, D.C.'s program is large and it is expanding. Because the D.C. program is so large, it allows other jurisdictions to see a program on a magnified scale. Based on D.C.'s large program, other jurisdictions can glean best practices and anticipate and mitigate challenges that arise in the creation of CCTV programs.

Second, Washington, D.C. experiences a unique threat; as the nation's capital it is home to some of the nation's most critical assets and infrastructure, therefore making it an obvious target for terrorist attacks and essential to protect in the event of natural disasters.[18] After the September 11, 2001 attack on the Pentagon, the D.C. government became even more acutely aware of the need for situational awareness and recommitted itself to the safety of its residents and tourists. Because D.C. stands to lose so much, it has dedicated much attention to, and generated a high level of expertise in, developing a superior public safety program. Its use of CCTV may serve to inform less experienced jurisdictions in developing their public safety programs, specifically with respect to the use of emerging CCTV technology.

Third, because of the legal structure governing the D.C. Homeland Security and Emergency Management Agency (HSEMA) regulation process, the D.C. CCTV program is subject to a heightened level of scrutiny; the program needs to (1) be efficient, both cost-wise and in delivering safety; and (2) be accepted by the Council of the District of Columbia

---

[17] *See* Greenberger, *supra* note 15.

[18] "The District of Columbia has been designated a high-threat target city by the U.S. Department of Homeland Security, and needs commensurate capabilities for preventing, mitigating and responding to terrorist attacks. These capabilities include risk-based strategic planning, threat and vulnerability analysis, and gap assessments." Homeland Security, Risk Reduction, and Preparedness Act of 2006 § 101(a) (D.C. 2006), *available at* http://www.dccouncil.washington.dc.us/images/00001/20061218162318.pdf. *See also* D.C. CODE §7-2205 (2010).

(Council) and their electorate.[19] HSEMA needed to gain permission to use the regulations, so the regulations needed to be carefully drafted to become palatable to more stakeholders—this is a check rarely imposed when jurisdictions draft CCTV regulations and implement programs. As a result, HSEMA's comments submitted on the CCTV regulations—and the input from the other commenting organizations—influenced the regulations considerably and were treated very seriously. Since D.C. works with more players at the table and more checks than many other jurisdictions, Washington, D.C.'s process can serve as an example to jurisdictions that need to adhere to more demanding procedures before implementing CCTV programs.

Finally, Washington, D.C. boasts a unique culture of politically involved, attentive residents who vigilantly watch and comment on issues in their community. This level of accountability required D.C. to build a strong program and communicate with the media to keep residents informed and allowed the agencies to benefit from active feedback. Other communities can benefit from this added perspective of heightened accountability and glean the best practices for responding to and addressing residents' inquiries and concerns.

B. The Legal Process Behind Washington, D.C.'s CCTV Program

The CCTV program in Washington, D.C. is defined by the city's exposure to risk and its unique culture. The risk of being the seat of the nation's government and home to so many critical assets drove the decision to use more than 5,200 cameras in its CCTV program.[20] Also, the emphasis the D.C. culture placed on the protection of civil liberties and privacy inspired the city's collaboration with the Constitution Project[21] in drafting the CCTV program's regulations.[22] Crime deterrence is certainly a priority to the District government, and inspiring confidence in the government's ability to serve and protect residents, workers, commuters, and particularly tourists was a critical factor in Washington, D.C.'s decision to bolster its CCTV

---

19 *Id.* § 2-505 (providing the process by which the regulations are reviewed and passed).

20 Press Release, *supra* note 16.

21 The Constitution Project is a politically independent think tank established in 1997 to promote and defend the fundamental tenets of our nation's founding document. On a wide range of matters, the Constitution Project assembles committees that span partisan divides, forging consensus and transforming it into bipartisan political coalitions and broader public support for safeguarding our Constitution. *See, e.g.*, CONSTITUTION PROJECT, THE USE AND ABUSE OF IMMIGRATION AUTHORITY AS A COUNTERTERRORISM TOOL: CONSTITUTIONAL AND POLICY CONSIDERATIONS vii (2008), *available at* http://www.constitutionproject.org/ manage/file/48.pdf.

22 D.C. MUN. REGS. tit. 24, § 2500 (2010).

program.[23] Much of the city's revenue is derived from tourism, and after the September 11, 2001 attack on the Pentagon the city needed to make every effort not only to ensure residents' and tourists' physical safety, but also to allow them to feel safe within the city.

Currently, D.C.'s CCTV program is divided into two separate parts that are governed by the same regulations. The Metropolitan Police Department's (MPD's) cameras feed only to police officers in an MPD building, and all other agencies' camera feeds stream to a fusion center located in a secured section of HSEMA's offices.[24] The regulations that MPD drafted with the Constitution Project currently govern both the MPD and HSEMA programs, although HSEMA has created several drafts of regulations to govern their interagency camera program aimed towards situational awareness.[25]

When HSEMA coordinated the D.C. agencies' video streaming from interoperable cameras, the purpose was slightly different than that of MPD's program. According to HSEMA:

> The mission of the D.C. Homeland Security and Emergency Management Agency is to manage the District's emergency operations, to *prevent*, respond to, and recover from natural and man-made emergencies.
>
> HSEMA coordinates all planning and preparedness efforts and generates a real-time common operating picture during events, to facilitate informed decision-making and response. This common operating picture achieves situational awareness and eliminates or minimizes conflicting information received from numerous sources.[26]

If technology is going to be used to a different end, the means may vary. Accordingly, HSEMA drafted regulations to govern (1) the operating procedures for the circumstances under which recording is permissible; (2) the treatment of other agencies' video feeds; and (3) the governance of employees monitoring the feeds.[27] MPD, in contrast, is the primary crime response agency and operates its own cameras without the assistance of other

---

[23] Telephone Interview with Steven Kral, Senior Policy Advisor, District of Columbia Homeland Security and Emergency Management Agency (Oct. 20, 2009) (on file with author).

[24] *Id.*

[25] *Id.*

[26] HOMELAND SEC. AND EMERGENCY MGMT. AGENCY, FY09 PERFORMANCE PLAN 1 (2009), *available at* http://capstat.oca.dc.gov/docs/fy09/HSEMA.pdf (emphasis added). *See also* D.C. CODE § 7-2205 (2010).

[27] Homeland Security and Emergency Management Agency, Use of Closed Circuit Television, 55 D.C. Reg. 25 at 006907 (June 20, 2008), *available at* http://newsroom.dc.gov/show.aspx?agency=os&section=37&release=14075&year=2008&month=6&file=file.aspx%2frelease%2f14075%2f09%2520-%2520%2520Emergency%2520Rulemaking%2520final.pdf.

agencies;[28] there are no novel issues or concerns about procedures for sharing information and privacy protections in the MPD context. Because HSEMA created a different kind of program than MPD, consolidated different agencies' employees and video feeds in the same room for the exact purpose of sharing information, and sought to gain situational awareness—which is more nuanced and encompasses more activity than merely monitoring criminal activity—the HSEMA program's regulations needed to be tailored accordingly.

The legal procedure for establishing CCTV regulations in Washington, D.C. is an anomaly in that the Council has the ability to delegate rulemaking authority to the executive branch while requiring that the drafted regulations be subject to Council review and even affirmative approval.[29] While the Council does not exercise this control over every agency or every set of regulations, it has subjected HSEMA's CCTV program regulations to this extensive process.[30] Once the agency that seeks to implement a program drafts its regulations, it publishes a Proposed Rule via the Executive Office of the Mayor for a thirty day public notice and comment period.[31] If comments regarding the program are significant and substantive, the agency amends the Proposed Rule and submits it for another thirty day notice and comment period.[32] If there are neither significant nor substantive comments, then the Executive Office of the Mayor submits the Proposed Rule to the Council for review.[33] The Council then has either thirty or forty-five days to review the Proposed Rule.[34] If the Council requires affirmative approval for a program's or an agency's regulations, as it did for HSEMA's CCTV program, then the regulations are ineffective until the Council approves them. If the allotted review period closes without the Council's express approval, the regulations remain ineffective.[35] If the Council grants affirmative approval—which has not happened for HSEMA's proposed CCTV regula-

---

[28] Interview with Steven Kral, *supra* note 23. *See also* District of Columbia Metropolitan Police Department, CCTV System Operations and Capabilities, http://mpdc.dc.gov/mpdc/cwp/view,a,1238,Q,541572,mpdcNav_GID,1545,mpdcNav,|31748|,.asp (last visited Mar. 11, 2010).

[29] This power held by the D.C. Council is derived from the Home Rule Act, which transferred all authorities of the former Commissioners to the current governing body. *See generally* D.C. CODE § 2-505; Home Rule Act, D.C. CODE §§ 1-203.02, 1-204.04, 1-303.01, 1-303.03 (1973).

[30] Interview with Steven Kral, *supra* note 23.

[31] *See* D.C. CODE § 2-505(a).

[32] *See id.*

[33] *See supra* note 29.

[34] *Id.*

[35] *Id.*

tions—then the regulations are published for notice and comment as a Final Rule.[36]

V. ADDRESSING OVERARCHING CONCERNS REGARDING CCTV POLICY

When HSEMA released its proposed regulations for its CCTV program, the submitted comments reflected the overarching concerns that are generally expressed over CCTV. Comments were submitted by the American Civil Liberties Union (ACLU) and the Constitution Project.[37] They focused their concerns on the constitutional implications and civil liberties issues that may arise with such a program, and HSEMA amended its Proposed Rule to assuage those concerns.[38]

Generally, when CCTV comes under public scrutiny, opponents express concerns about CCTV technology's capabilities as a threat to people's Fourth Amendment rights. However, CCTV programs do not implicate the Fourth Amendment, as no person moving about public spaces has a reasonable expectation of privacy.[39] Government CCTV programs are established by placing cameras on public property—for example, on a lamp post—with a view of public space. Anyone viewing CCTV cameras can only view what a police officer on foot, or any person on the street, would be able to see. As technology develops, jurisdictions are able to purchase and place cameras throughout the area with pan-tilt-zoom capabilities, but a properly regulated CCTV program takes into consideration that any information gathered by viewing areas that are not in plain view or in public space would not be able to be used in any sort of a criminal investigation, and would ensure that cameras are not placed in questionable areas.[40] To be

---

[36] *Id.*

[37] The ACLU's and the Constitution Project's submitted written comments (July 21, 2008, November 26, 2008, and July 17, 2008, respectively) on HSEMA's proposed rule are not published but may be accessed by sending a written request to HSEMA's Public Information Officer.

[38] These regulations are unpublished but may be accessed through a written request. *See id.*

[39] "For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Katz v. United States, 389 U.S. 347, 351 (1967).

[40] In this way, cameras effectively function as a police officer would. In the unlikely instance that a suit is brought based on a Fourth Amendment violation claim, a court may find that, like binoculars and flashlights, the camera is just another technological development that simply enhances plain view, only in this case an officer or a government employee viewing the video feed would be able to see whatever an officer there on the street would see. In fact, the very purpose of a CCTV program is to be more efficient than to try to have an officer in all places at all times to see what could be viewed by one officer monitoring several video feeds.

even more transparent, the current trend in implementing CCTV program policy is to post publicly that an area is subject to video surveillance. In certain areas of Baltimore, signs are posted in monitored areas, while in Washington, D.C. HSEMA posts all locations of CCTV cameras on its website.[41] HSEMA's program thus allows people to research exactly where cameras are before they leave the house and to be aware of when and where they are monitored. For these reasons, Fourth Amendment privacy concerns should not hinder or in any way influence the implementation of a CCTV program.

Critics' other constitutional concerns stem from the First Amendment, but CCTV programs should not infringe on these rights either. Certain interest groups have expressed concern that CCTV technology may allow government employees to focus cameras on groups assembling in public places, or zoom in on pamphlets or other literature that people carry, effectively hindering people's willingness to exercise their right to assemble or carry and distribute literature.[42] However, regulations governing CCTV programs should expressly specify that any such targeting of people and their behavior, or zooming in on their pamphlets or other literature, is prohibited. Thus, CCTV programs in and of themselves should neither pose a threat to, nor hinder, people's willingness to exercise their First Amendment rights. Any constitutional issues raised would be marked by misuse of the program, which is in no way distinguishable from misuse of any other government program that results in constitutional violations.

When HSEMA put its Proposed Rule out for comment, the ACLU and the Constitution Project responded with comments[43] that paralleled the content of a Fall 2006 New York Civil Liberties Union (NYCLU) report.[44] In Fall 2006, the NYCLU issued a special report entitled *Who's Watching? Video Camera Surveillance in New York City and the Need for Public Oversight*.[45] The report provides examples of circumstances under which some citizens might not want to be observed, much less recorded.[46] According to the report, the NYCLU was primarily concerned that such a surveillance system would effectively "undermin[e] fundamental rights of privacy, speech, expression and association."[47]

---

41 District of Columbia, Closed Circuit Television (CCTV)—Situational Awareness, http://dcema.dc.gov/dcema/cwp/view,a,1225,q,644339.asp (last visited Mar. 11, 2010).

42 *See, e.g.*, *supra* note 37.

43 *Id.*

44 *See generally* NYCLU REPORT, *supra* note 6.

45 *Id.*

46 *Id.* at 1.

47 *Id.*

The NYCLU report includes a very helpful list of elements that should be considered when jurisdictions draft regulations governing their CCTV programs. The report includes the concerns that residents have and provides the academic perspective.[48] The report is the most comprehensive guide that agencies can use to anticipate obstacles and work to find a compromise that inspires faith in government but maintains the capabilities of an effective CCTV program.

First, the NYCLU suggests that jurisdictions state clear goals and purposes for CCTV programs.[49] These goals should be based on a needs assessment performed before the cameras are installed and justified by periodic audits of the efficacy of the cameras' placements and adherence to the program's regulations.[50] Second, the report calls for public notice of the program, the location of the cameras, and the proposed locations for additional cameras so that the community may comment.[51] Third, the NYCLU emphasizes that the regulations should require a training program and a system for vigilant supervision of the government employees tasked with monitoring the video feeds.[52] Fourth, a jurisdiction's regulations should explicitly state the recording, storing, and disposal policies for the videos, including the exact length of time permissible to keep a recording; additionally, the NYCLU recommends that this section of the regulations address the circumstances under which recordings will be accessible and disseminated.[53]

The NYCLU report devotes much attention to its fifth suggested section, prohibition and penalties.[54] This section clearly defines what activity would constitute a misuse of CCTV technology, such as zooming in on fliers or pamphlets "being distributed or carried pursuant to First Amendment rights,"[55] and "target[ing] or observ[ing] individuals based upon race, gender, ethnicity, sexual orientation, disability, or other classifications protected by law."[56] The fifth section cautions that cameras observe only public areas where people enjoy no reasonable expectation of privacy, and recommends that cameras must not have any audio capabilities.[57] The lack of audio capabilities is very important to agencies designing CCTV programs

48 *See generally id.*

49 *Id.* at 13–16.

50 *Id.* at 13.

51 *Id.* at 13–14.

52 *Id.* at 14–15.

53 *Id.* at 15–16.

54 *Id.* at 16.

55 *Id.*

56 *Id.*

57 *Id.*

and for interest groups alike, and must be stated in the regulations, as well as emphasized in town hall meetings and media releases.

HSEMA's most recent amendments to its Proposed Rule reflect all of the recommendations outlined in the NYCLU report and the comments HSEMA received.[58] Though HSEMA's amended regulations have not been affirmatively accepted by the Council, all CCTV cameras are currently governed by MPD's regulations, which were drafted with active participation from the Constitution Project, and delineate the same elements.[59]

VI. CURRENT GOVERNING REGULATIONS AND THEIR IMPLICATIONS

MPD's regulations,[60] drafted collaboratively with the Constitution Project, serve the ultimate goal of traditional police powers and public safety response. All CCTV camera feeds are currently governed by these MPD regulations. Initially, MPD policy section 2500 appears to focus on achieving situational awareness, which is one HSEMA's most critical functions. Section 2500.2 reads, "MPD's CCTV system is generally intended to be used: (1) to help manage public resources during major public events and demonstrations; (2) to coordinate traffic control on an as-needed basis; and (3) to combat crime as authorized by § 2508."[61] Section 2508.1 provides that "[t]he Chief of Police is authorized to use the CCTV system for the purpose of *preventing, detecting, deterring*, and investigating crime in neighborhoods in the District of Columbia."[62] This section's language appears to permit the mitigation aspect of HSEMA's mission, and should be interpreted to allow HSEMA to create a common operating picture[63] to enhance safety and stay abreast of action in critical, high-risk, or high-threat areas. Section 2501.2 addresses the sentiment that a video surveillance system may not be as effective as having officers patrol the street. This section states that "[t]he technology will not be used to replace current policing techniques."[64] Otherwise stated, CCTV bolsters current safety programs rather than replacing them.

After MPD's regulations address the purpose of its CCTV program, they outline the policy governing it. The Council accepted MPD's CCTV regulations in large part because of the Constitution Project's heavy influence in drafting this section; not only is this one of the D.C. program's greatest strengths, but also it provides a blueprint for other jurisdictions

---

58 Interview with Steven Kral, *supra* note 23.

59 *See* D.C. MUN. REGS. tit. 24, § 2501 (2010).

60 *Id.* § 2500.

61 *Id.* §2500.2.

62 *Id.* §2508.1 (emphasis added).

63 *Supra* note 5.

64 D.C. MUN. REGS. tit. 24, § 2501.2.

attempting to draft regulations acceptable to civil liberties interest groups. The following sections directly reflect the guidelines from the NYCLU and the Constitution Project's comments.

> 2501.3 Under no circumstances shall the CCTV systems be used for the purpose of infringing upon First Amendment rights.
>
> 2501.4 Operators of the CCTV systems shall not target/observe individuals solely because of their race, gender, ethnicity, sexual orientation, disability or other classifications protected by law.
>
> 2501.5 CCTV systems shall be used to observe locations that are in public view and where there is no reasonable expectation of privacy.
>
> 2501.6 MPD shall not use audio in conjunction with the CCTV unless appropriate court orders are obtained.
>
> 2502.8 On a semi-annual basis, MPD will provide updates on the CCTV system at community meetings to be announced to the public.
>
> 2502.9 MPD will provide information about the CCTV system and its usage in its Annual Report. The information shall include the viewing area of cameras, periods of activation and/or recording and the purposes of activation and recording, disposition of any recordings, and an evaluation of whether the camera achieved the purposes stated in section 2500. The MPD shall not include any information pertaining to cameras deployed pursuant to a court order or deployed as part of an on-going criminal investigation.
>
> 2504.4 Operators of CCTV systems shall not focus on hand bills, fliers, etc., being distributed or carried pursuant to First Amendment rights.
>
> 2507.1 MPD's Office of Professional Responsibility will conduct periodic audits, at least quarterly, to ensure compliance with these regulations.
>
> 2507.2 The audits conducted pursuant to 2507.1 shall be provided to the Mayor and the Council of the District of Columbia.[65]

The Operator Certification and Activation and Usage sections of the MPD regulations address the sensitive subject of who views the footage and how they do so. The regulations require the certification of all program operators and provide that "[a]ll operators of the CCTV systems shall sign a certification that they have read and understand the CCTV regulations and acknowledge the potential criminal and/or administrative sanctions for unauthorized use or misuse of the CCTV systems."[66] The regulations further state that:

> Anyone who engages in the unauthorized use or misuse of CCTV systems shall be subject to criminal prosecution and/or administrative sanctions, including termination. The administrative sanctions will depend on the se-

---

65 *Id.* §§ 2501.3–.6, 2502.8–.9, 2504.4, 2507.1–.2.

66 *Id.* § 2503.2.

> verity of the infraction and shall be taken in accordance with MPD's Disciplinary Procedures and Policies General Order and/or the adverse and corrective action procedures as provided in the District Personnel Manual.[67]

Recording policies are another focal point in developing CCTV policy. The circumstances under which the footage is permitted to be recorded and the storage of such tapes may garner much attention from the media, residents, and public interest groups, so agencies must be transparent with the program's policies and be prepared to justify them. "Except in exigent circumstances or when recording is being done pursuant to a court order, the Chief of Police shall issue written authorization prior to recording any CCTV feed."[68] Additionally, MPD's regulations require documentation for every recording: "[t]he record shall include a copy of any written authorizations pertaining to each period of recording, the name(s) of any person(s) recording, a general description of the activity being recorded, and documentation as to when the recording began and ended."[69] If a recording is justified by exigent circumstances, documentation must describe "the exigency that gave rise to the need to record without prior written authorization."[70]

Any footage that is recorded pursuant to a CCTV program must be handled vigilantly; security is critical so as not to create civil liberties infractions. Agencies must limit their retention of recordings, since indefinite retention of tapes that do not arouse suspicion is unreasonable. The MPD regulations cap retention at "10 business days after which time they will be recorded over or destroyed."[71] If the footage "contain[s] evidence of criminal activity, because the recordings capture an occurrence that may subject MPD to civil liability, or because the recording will be used for training purposes," then it may be retained longer than ten business days.[72] "Recordings that contain evidence of criminal activity or recordings that capture an occurrence that may subject MPD to civil liability shall be maintained to final case disposition."[73] The regulations require extensive documentation whenever such recordings are retained beyond the standard ten business day period.[74]

---

67 *Id.* § 2503.3.

68 *Id.* § 2505.1.

69 *Id.* § 2505.2.

70 *Id.* § 2505.3.

71 *Id.* § 2505.5.

72 *Id.* § 2505.6.

73 *Id.*

74 *Id.* §§ 2505.7–2505.8.

With respect to the public notice issue, MPD's regulations allow the public an opportunity to be heard, but vest the ultimate authority to add and place cameras in the Chief of Police. Section 2502.7 provides that "MPD will post and maintain signage"[75] and section 2502.4 clearly empowers the Chief of Police by requiring that "[t]he Chief of Police shall consider the comments submitted by the public in determining whether to go forward with deployment of the camera. The Chief of Police will provide public notice of his decision and provide an explanation."[76] Ultimately, there is no further check on this authority; the Chief of Police's explanation could be as simple as, "this will protect you, and does not violate any of your rights, so if MPD does not place a camera at [a location at issue], the agency is not performing due diligence." Vesting such final decision making authority in the Chief of Police is unlikely to cause additional public concern, as people who oppose this grant of authority are likely to object to CCTV programs as a whole, and will not distinguish an additional camera from the existing program.

VII. GAPS CAUSED BY USING REGULATIONS NOT DRAFTED FOR A UNIQUE PROGRAM

The MPD regulations' Public Notification section,[77] along with several others,[78] underscores the gaps that remain in a policy governed by regulations that were written before the program was fully formed. The section of the MPD regulations vesting authority in the Chief of Police raises the following question: If HSEMA operates its consolidation of interagency cameras under these MPD regulations, in whom is this authority vested—surely not the Chief of Police? It would be logical to infer that, since the Chief of Police is the director of MPD, and since the MPD regulations were

---

[75] *Id.* § 2502.7.

[76] *Id.* § 2502.4.

[77] *Id.* § 2502.

[78] *See, e.g.*, *id.* § 2506.1 ("MPD shall be responsible for the safekeeping, maintenance and servicing of MPD equipment (e.g., cameras, cables, monitors, recorders, etc.).)"; *id.* § 2507.1 ("MPD's Office of Professional Responsibility will conduct periodic audits, at least quarterly, to ensure compliance with these regulations."); *id.* § 2503.3.

> Anyone who engages in the unauthorized use or misuse of CCTV systems shall be subject to criminal prosecution and/or administrative sanctions, including termination. The administrative sanctions will depend on the severity of the infraction and shall be taken in accordance with MPD's Disciplinary Procedures and Policies General Order and/or the adverse and corrective action procedures as provided in the District Personnel Manual.

Id.; *id.* § 2505.6 ("Recordings that contain evidence of criminal activity or recordings that capture an occurrence that may subject MPD to civil liability shall be maintained to final case disposition.").

originally drafted to govern the program that MPD designed and oversaw, the authority with which the regulations provide the Chief of Police should apply to the director of the agency implementing the program—in this case, the director of HSEMA. However, some ambiguity remains because this issue is not directly addressed by MPD's regulations, which were drafted specifically for its program and not HSEMA's.

The MPD regulations' references to the Chief of Police comprise one of the many outstanding issues that remain with applying these regulations to HSEMA's CCTV program. As strong as the MPD regulations are, they leave something to be desired when they are applied to the HSEMA-coordinated interagency CCTV program because they were not crafted specifically for the program HSEMA has designed. Requiring HSEMA and its system of interagency camera monitoring to operate under MPD's regulations is further complicated by section 2508.4, which reads, "[w]hen CCTV is used to combat crime, recordings may be *passively monitored*, meaning that the video feeds *may not be monitored in real time*, and recordings may be viewed by MPD personnel *where there is reason to believe that the viewing may help solve a crime*."[79] This provision entirely undermines HSEMA's objective to create situational awareness and mitigate any developing threat. While proscribing active monitoring may be entirely appropriate for police cameras, which serve a distinctly different purpose and are excluded from the collaborative HSEMA program, it is fundamentally inappropriate to hold HSEMA's program to this active-monitoring restriction when HSEMA, because of Washington, D.C.'s heightened risk, has been tasked with maintaining situational awareness. Passive monitoring and the use of recordings to solve crimes indicate a clearly reactive role; by definition, one can only solve a crime that has already been committed. The language in section 2508.4 dramatically limits HSEMA's ability to fulfill its responsibility to mitigate developing situations and disregards any responsibility to monitor developing natural disasters. Though the language successfully establishes an effective MPD camera program, it does not serve HSEMA's purposes. The two distinct programs require separate regulations. The language in the MPD regulations directly serves a police program and directly interferes with HSEMA's mission to maintain awareness to preempt incidents.

The current saving grace for HSEMA's program lies in section 2500.3, which reads, "[i]n addition to the purposes listed in 2500.2, the CCTV system may also be employed in exigent circumstances for the duration of the exigent event or circumstance."[80] One could argue that ever since September 11, 2001, the nation's capital has been in an ongoing state of

---

79 *Id.* § 2508.4 (emphasis added).

80 *Id.* § 2500.3.

vigilance. As the seat of the American government and home to so many terrorist targets, D.C. is arguably in a constantly exigent circumstance (as distinguished from another city of similar size).

Three salient inconsistencies regarding D.C.'s CCTV program remain and need to be addressed in order to have a solid and transparent program. These are issues that are not unique to Washington, D.C. but need to be considered for any program aiming to achieve situational awareness through a shared, interagency network of camera feeds.

First, the responsibility for storage and security of recorded footage needs to be clarified—either the coordinating agency (in Washington, D.C., HSEMA) must handle this or each agency must be responsible for its own camera feeds.

Second, MPD's reference to "exigent circumstances" is a nebulous concept; one could argue that the definition of exigency is influenced by the mission of the agency and of the program. Agencies serve different roles and therefore have different priorities. An exigent circumstance (warranting recording and retaining the footage) for a police department with specific objectives may be different than what constitutes an exigent circumstance for an emergency management and homeland security program. Situational awareness is a much more nuanced goal, and it is informed by many different elements of activity within a city. Ignoring these nuances, or ignoring that exigency may be defined by the perspective and the role with which an agency approaches a situation, at best adds a level of opaqueness to the regulations and at worst limits an important agency's delivery of a critical government service. It is wasteful and dangerous to limit execution of a government program based upon poorly worded or thought-out regulations

Third, MPD's regulations fall short due to section 2503.1, "[o]nly certified operators shall operate the CCTV system."[81] A regulation requiring any employee who monitors the CCTV cameras to be certified, without identifying some structure or criteria for certification, is utterly unquantifiable and essentially meaningless. "Certification" could mean nothing more than a stamp on a stack of unread papers. Without recreating the Napoleonic Code, programs would be stronger and civil liberties would be more robustly protected with more guidelines or standards included when requiring certification. Enough jurisdictions have created templates for such training and vetting programs as to make this a realistic, rather than an unduly burdensome, addition to a jurisdiction's regulations.

Careful examination of the way Washington, D.C. has structured and implemented its CCTV program should reinforce the importance of clearly identifying the purpose for a city's CCTV programs and producing regulations tailored to achieve that goal.

---

81 *Id.* § 2503.1.

VIII. THE WAY FORWARD

For CCTV technology to be used most effectively, it must be used efficiently while maintaining people's faith in government—faith that they are safe, that their taxes are being spent on programs that enhance public safety, and that their civil liberties are not being compromised in the process. To craft the best policy for a CCTV program, and to present the best argument and the most accurate picture of the technology's ability to serve public safety needs (which is critical for jurisdictions in which the initiating agency needs approval of regulations from a separate governing body), an agency must clearly identify its program's purpose, its goals, and the steps it will take to implement them. The regulations must be transparent and overt, and must include language to protect civil liberties in an effort to address the concerns regarding misuse of CCTV technology. The agency must identify the reasons as to why their goals cannot be better served in a seemingly less pervasive or less expensive way. Although agencies must tailor the policy to their unique programs, they should look to leading authorities on civil liberties and existing CCTV programs for best practices.

Finally, agencies must prepare for the peripheral impact that a CCTV program carries. Citizens may make Freedom of Information Act requests for recorded CCTV footage, and attorneys may subpoena either recordings or government employees who watched an incident unfold on a CCTV monitor. Such requests may be made under federal or state law, and may be made for criminal or civil litigation purposes.[82] To maintain the integrity of a CCTV program, and to use it truly for the most noble and essential safety purposes, there must be a way to protect such footage from use in trivial civil litigation. It is unlikely that a municipality's homeland security agency regulations will override the laws governing such requests, but the agency has a responsibility to maintain the privacy protections ensured by the regulations governing the program.

Along the same vein, agencies will need to work together to implement an effective CCTV program. Financial decisions concerning the technology to be purchased and questions regarding distribution of authority and human resources may arise when members of different agencies are deployed to a fusion center. A municipality may need to update its building code when it implements the CCTV program; if cameras are placed strategically, and then a new structure is built that impedes the CCTV camera's access to a critical asset, there must be a way to ensure that another camera can be placed even if the new building is privately owned. In these respects, as in others, implementing an effective CCTV program is an interagency

---

82 *See generally* Freedom of Information Act, 5 U.S.C. § 552 (2006).

undertaking. Jurisdictions must be prepared to address these peripheral issues if the technology is to be used successfully.

CCTV programs can only become stronger and more effective as jurisdictions share information with each other and with the community. By analyzing existing CCTV programs, seriously considering comments and concerns, and crafting effective yet sensitive programs, agencies can fully perform their most essential task: enhancing public safety while protecting civil liberties. In this way, CCTV programs can build safer communities.